

- 32 -

CLAIMS

1. A protocol for entering, disabling/erasing  
5 scrambled data access rights transmitted from a  
transmission center to at least one descrambling  
terminal to which is linked an access control  
module equipped with a security processor, these  
access rights being entered in said access control  
10 module, said scrambled data being subjected to an  
access control by periodic transmission of access  
control messages, conveying access criteria and a  
cryptogram of a control word that is changed  
periodically and encrypted using an operation key,  
15 then, in each security processor, conditionally  
upon verifying the true value of at least one  
entered access right against said access criteria,  
by decrypting the cryptogram of the control word  
using said operation key, transmitting the  
20 restored control word to the descrambling terminal  
and descrambling said scrambled data using said  
restored control word, characterized in that it  
consists at least in:
- forming any access right entered in said access  
25 control module as a set of independent variables  
and linked variables comprising at least, in  
addition to an access right identification  
variable, an entered access right action date  
variable and a status variable which can have  
one of three encoded values signifying access  
30 right enabled, access right disabled, access  
right erased;
  - transmitting from said transmission center to  
each descrambling terminal and to the access  
control module linked to the latter at least one  
35 access right management message, said message  
comprising at least, in addition to an entered  
access right identification variable, an action

- 33 -

- 5        date variable and a status assignment variable,  
the encoded value corresponding to an enabled  
access right, a disabled access right or an  
erased access right; and on receipt of said  
access right management message, at said access  
control module,
- 10        - assigning said action date to the entered access  
right corresponding to the access right  
identification variable of said access right  
management message, and
- 15        - allocating said status assignment variable  
corresponding to an enabled access right, a  
disabled access right or an erased access right  
to said status variable of said corresponding  
entered access right.
2.       The protocol as claimed in claim 1, characterized  
in that, for an operation to enter a defined  
access right in an access control module, said  
20       action date variable of said access right  
management message corresponds to an entry date,  
and the status assignment variable is an encoded  
value corresponding to an enabled right, the entry  
operation consisting in entering, into said access  
25       control module, a defined access right, the action  
date of which is that of said entry date and for  
which the status variable is that of said status  
variable and corresponds to an enabled right.
- 30       3.       The protocol as claimed in claim 2, characterized  
in that, prior to the entry operation proper of  
said defined access right, the latter consists in  
addition, in said access control module,
- 35       - in verifying the existence, in said access  
control module, of an entered access right  
corresponding to said defined access right and  
for which the status variable corresponds to the

- 34 -

encoded value signifying right enabled or right disabled, and on a positive response to said verification:

- 5       - in verifying the posteriority nature of said action date variable corresponding to an entry date in relation to the action date of said identical access right and on a positive response to said posteriority nature verification,
- 10       - performing an update of said action date variable of said identical access right, based on said action date corresponding to an entry date,
- 15       - assigning, to said status variable of said identical access right, the encoded value corresponding to an enabled right, allowing said entered access right to be enabled.

4.     The protocol as claimed in claim 2 or 3,  
20     characterized in that, on a negative response to said verification of the existence of an identical access right, the latter consists in addition in performing an update by first entry of this access right, for which the action date corresponds to  
25     the entry date.

5.     The protocol as claimed in claim 1, characterized in that, for an operation to disable an access right entered in an access control module, said  
30     action date variable of said access right management message corresponds to a disabling date and the status assignment variable is an encoded value corresponding to a disabled right, the disabling operation consisting in assigning, to  
35     said status variable of said entered access right, said encoded value corresponding to a disabled

- 35 -

right and updating said action date of said entered access right based on said disabling date.

- 5 6. The protocol as claimed in claim 5, characterized in that, prior to the disabling operation proper, the latter consists in:
- verifying the existence, on said access control module, of an entered access right corresponding to said access right of said management message;
  - 10 - verifying the posteriority nature of said action date variable corresponding to a disabling date with respect to said action date variable of said entered right.
- 15 7. The protocol as claimed in one of the preceding claims, characterized in that, for any status assignment variable of the management message corresponding to an erased access right and for any access right entered in the access control module for which the status variable corresponds to an enabled right or a disabled right, the latter consists at least in:
- an update of the action date of said entered right;
  - 25 - an allocation, to said status variable of said entered access right, of said status assignment variable of the management message corresponding to an erased access right, said allocation operation forming, for said entered access right, a virtual erasure operation.
- 30
8. The protocol as claimed in claim 7, characterized in that the update and virtual erasure steps of said entered access right are preceded by a step to verify the existence, on said access control module, of an entered access right corresponding to said access right of said management message,
- 35

- 36 -

and a step to verify the posteriority of said action date variable of said management message with respect to said action date variable of said entered access right.

5

9. The protocol as claimed in one of claims 7 or 8, characterized in that said virtual erasure operation is followed by a physical erasure operation of said access right.

10

10. The protocol as claimed in claim 9, characterized in that said physical erasure operation is immediate or deferred.

15

11. The protocol as claimed in one of claims 2 or 3, characterized in that, for an entered access right for which the status assignment variable corresponds to an erased access right, the latter also consists in performing an update by first entry of this access right, said access right being assigned a status variable corresponding to an enabled right and for which the action date corresponds to the entry date.

20

12. The protocol as claimed in one of claims 5 or 6, characterized in that, for an entered access right for which the status assignment variable corresponds to an erased access right, the latter also consists in performing an update by first entry of this access right, said access right being assigned a status variable corresponding to a disabled right and for which the action date corresponds to the entry date.

30

13. The protocol as claimed in one of claims 5 or 6, characterized in that, on a negative response to said verification of the existence of a

35

- 37 -

corresponding access right, the latter also consists in performing an update by first entry of this access right, for which the action date corresponds to a disabling date, said access right being assigned a status variable corresponding to a disabled right.

14. A module controlling access to scrambled data transmitted from a transmission center to at least one descrambling terminal to which is linked this access control module, characterized in that it comprises, entered in the memory of this access control module, at least one access right formed by a set of independent variables and of linked variables, comprising at least, in addition to an entered access right identification variable and a validity dates variable, an entered access right action date variable and a status variable that can have one of three encoded values signifying access right enabled, access right disabled or access right erased.

15. The access control module as claimed in claim 14, characterized in that since said access control module comprises a microprocessor card fitted with a security processor and a secured non-volatile programmable memory, said at least one access right is entered in said secured non-volatile programmable memory.

16. The access control module as claimed in claim 14 or 15, characterized in that, for an access control to scrambled data for a pay television service, said access rights cover said access rights defining the modes of access to said scrambled data and electronic purses allocated to

- 38 -

the subscribing user, the holder of said access control module.